

WITT VECTOR RINGS AND QUOTIENTS OF MONOID ALGEBRAS

Sina Ghassemi-Tabar

ABSTRACT. In a previous paper Cuntz and Deninger introduced the ring $C(R)$ for a perfect \mathbb{F}_p -algebra R . The ring $C(R)$ is canonically isomorphic to the p -typical Witt ring $W(R)$. In fact there exist canonical isomorphisms $\alpha_n: \mathbb{Z}R/I^n \xrightarrow{\sim} W_n(R)$. In this paper we give explicit descriptions of the isomorphisms α_n for $n \geq 2$ if $p \geq n$.

1 Introduction

For a perfect \mathbb{F}_p -algebra R consider the monoid algebra $\mathbb{Z}R$ where R is viewed as a monoid under multiplication. In [1] the ring $C(R)$ is constructed as the I -adic completion of $\mathbb{Z}R$ where I is the kernel of the natural projection $\pi: \mathbb{Z}R \rightarrow R$. It turns out that $C(R)$ is a strict p -ring with $C(R)/pC(R) = R$ and therefore canonically isomorphic to the ring of p -typical Witt vectors of R . As an immediate consequence we have a unique isomorphism $\alpha_n: \mathbb{Z}R/I^n \xrightarrow{\sim} W_n(R)$ for every $n \geq 2$, c.f. [1] Remark 6 and Corollary 7. In [1] there is an explicit description of the isomorphism $\alpha_2: \mathbb{Z}R/I^2 \xrightarrow{\sim} W_2(R)$. It was verified by using addition and multiplication on the truncated Witt ring $W_2(R)$ to prove that α_2 is a homomorphism and to conclude that it has to be the unique isomorphism. We choose another approach to calculate the isomorphism α_n by using the inverse map $\beta_n: W_n(R) \xrightarrow{\sim} \mathbb{Z}R/I^n$ given by the formula

$$\beta_n(r_0, r_1, \dots, r_{n-1}) = \sum_{k=0}^{n-1} p^k [\phi^{-k}(r_k)] \bmod I^n \quad (1)$$

where ϕ is the Frobenius automorphism on R , c.f. [2] Corollary 6.5, [5] II §5. For background on the classical theory of Witt vectors see [3], [4]. I would like to thank C. Deninger for suggesting the topic of this note and for helpful discussions.

2 Determination of the isomorphism α_n

Let R be a perfect \mathbb{F}_p -algebra. Consider the map $\phi: \mathbb{Z}R \rightarrow \mathbb{Z}R$, $\sum n_r[r] \mapsto \sum n_r[r^p]$. We have $\phi(x) \equiv x^p \bmod p\mathbb{Z}R$ for $x \in \mathbb{Z}R$. Therefore we can introduce the “arithmetic derivation”

$$\delta: \mathbb{Z}R \rightarrow \mathbb{Z}R, \quad x \mapsto \frac{1}{p}(\phi(x) - x^p).$$

We mention some immediate facts about δ .

Proposition 1 ([1] page 2). *For $x, y, x_1, \dots, x_n \in \mathbb{Z}R$ we have:*

(i)

$$\delta(x + y) = \delta(x) + \delta(y) - \sum_{k=1}^{p-1} \frac{1}{p} \binom{p}{k} x^k y^{p-k} \quad (2)$$

(ii)

$$\delta(xy) = \delta(x)\phi(y) + x^p\delta(y) \quad (3)$$

(iii)

$$\delta(x_1 \cdots x_n) = \sum_{k=1}^n x_1^p \cdots x_{k-1}^p \delta(x_k) \phi(x_{k+1}) \cdots \phi(x_n)$$

(iv)

$$\delta(x + y) \equiv \delta(x) + \delta(y) \pmod{I^n} \quad \text{if } x \in I^n \text{ or } y \in I^n \quad (4)$$

(v)

$$\delta(I^n) \subset I^{n-1} \quad \text{for } n \geq 1 \quad (5)$$

With these properties we are able to derive equations which will be useful for determining the map α_n above.

Lemma 2. *For $a, b, c \in \mathbb{Z}R$ we get:*

(i)

$$a \equiv b \pmod{I^n} \Rightarrow \delta(a) \equiv \delta(b) \pmod{I^{n-1}} \quad (6)$$

(ii)

$$a \equiv b + c \pmod{I^n} \text{ and } c \in I^{n-1} \Rightarrow \delta(a) \equiv \delta(b) + \delta(c) \pmod{I^{n-1}} \quad (7)$$

(iii)

$$ab \in I^n \Rightarrow \delta(a + b) \equiv \delta(a) + \delta(b) \pmod{I^n} \quad (8)$$

(iv)

$$\delta(p) \equiv 1 \pmod{I^{p-1}} \quad (9)$$

(v)

$$\delta(pa) \equiv \phi(a) \pmod{I^{p-1}}$$

In particular

$$\delta(pa) \equiv \phi(a) \pmod{I^k} \quad \text{for all } 0 < k < p. \quad (10)$$

Proof. (i) For $y \in I^n$ we have by using equations (4) and (5)

$$a = b + y \Rightarrow \delta(a) = \delta(b + y) \equiv \delta(b) + \delta(y) \bmod I^n \equiv \delta(b) \bmod I^{n-1}$$

since $\delta(y) \in I^{n-1}$ and $I^n \subseteq I^{n-1}$.

(ii) For $c \in I^{n-1}$ we have by using equations (4) and (6)

$$a \equiv b + c \bmod I^n \stackrel{(6)}{\Rightarrow} \delta(a) \equiv \delta(b + c) \bmod I^{n-1} \stackrel{(4)}{\equiv} \delta(b) + \delta(c) \bmod I^{n-1}.$$

(iii) The assertion follows from equation (2) because for $1 \leq k \leq p-1$ every binomial coefficient $\binom{p}{k}$ is divisible by p .

(iv)

$$\delta(p) = \delta(p \cdot 1) = \delta(p[1]) = [1] - p^{p-1}[1] \equiv [1] \bmod I^{p-1} \equiv 1 \bmod I^{p-1}$$

(v)

$$\delta(pa) \stackrel{(3)}{=} \delta(p)\phi(a) + p^p\delta(a) \equiv \delta(p)\phi(a) \bmod I^{p-1} \stackrel{(9)}{=} \phi(a) \bmod I^{p-1}$$

□

As already mentioned, our aim is to describe the isomorphisms $\alpha_n: \mathbb{Z}R/I^n \xrightarrow{\sim} W_n(R)$ for $n \in \mathbb{N}$ by explicit formulas. We begin with the case $n = 2$ to clarify the method.

Determining the isomorphism α_2

We obtain an explicit formula for the isomorphism $\alpha_2: \mathbb{Z}R/I^2 \xrightarrow{\sim} W_2(R)$ by using the inverse map β_2 and the arithmetic derivation δ . Because of formula (1) we know that for every element $x \in \mathbb{Z}R/I^2$ there exist uniquely determined elements $r_0, r_1 \in R$ with

$$x = \beta_2(r_0, r_1) = [r_0] + p[\phi^{-1}(r_1)] \bmod I^2 \quad \text{and} \quad \alpha_2(x) = (r_0, r_1).$$

Note here that $p \in I$ since R is an \mathbb{F}_p -algebra. So by reducing the first equation modulo I we obtain $x \equiv [r_0] \bmod I$ in $\mathbb{Z}R$ and therefore $r_0 = \pi(x)$. Substituting $\pi(x)$ for r_0 in the above equation, we have the identity

$$x \equiv [\pi(x)] + p[\phi^{-1}(r_1)] \bmod I^2.$$

The remaining component r_1 can now be determined by applying δ . We define a to be $a := \phi^{-1}(r_1)$. By applying δ to the second term on the right-hand side we have

$$\delta(p[a]) = \frac{1}{p}(\phi(p[a]) - (p[a])^p) = \frac{1}{p}(p[a^p] - p^p[a]^p) = [a^p] - p^{p-1}[a]^p.$$

Since $p - 1 \geq 1$ and $\delta([\cdot]) = 0$ we obtain the following congruence:

$$\delta(x) \stackrel{(7)}{\equiv} \delta([\pi(x)]) + \delta(p[a]) \bmod I \equiv \delta(p[a]) \bmod I \equiv [a^p] \bmod I \equiv [r_1] \bmod I$$

So for any element $y \in I$ satisfying $\delta(x) = [r_1] + y$ we obtain

$$\pi(\delta(x)) = \pi([r_1] + y) = \pi([r_1]) + \pi(y) = \pi([r_1]) = r_1$$

since I is the kernel of the natural projection π . In conclusion, the isomorphism α_2 is given by the formula

$$\alpha_2(x) = (\pi(x), \pi(\delta(x))). \quad (11)$$

As mentioned earlier, [1] Proposition 8 uses a different approach to obtain this formula.

Determining the isomorphism α_3

As already described we have

$$x \equiv [r_0] + p[\phi^{-1}(r_1)] + p^2[\phi^{-2}(r_2)] \bmod I^3$$

with uniquely determined elements $r_0, r_1, r_2 \in R$. By reducing modulo I^2 we obtain analogue results as above for r_0 and r_1 . So we can focus on calculating the component r_2 . Therefore we apply δ two times. Using equation (7) leads to the congruences

$$\begin{aligned} x - [r_0] &\equiv p[\phi^{-1}(r_1)] + p^2[\phi^{-2}(r_2)] \bmod I^3 \\ (7) \Rightarrow \delta(x - [r_0]) &\equiv \delta(p[\phi^{-1}(r_1)]) + \delta(p^2[\phi^{-2}(r_2)]) \bmod I^2 \\ &\Rightarrow \delta(x - [r_0]) \equiv [r_1] - p^{p-1}[r_1] + p[\phi^{-1}(r_2)] - p^{2p-1}[\phi^{-1}(r_2)] \bmod I^2 \\ 2p - 1 > 2 &\Rightarrow \delta(x - [r_0]) \equiv [r_1] - p^{p-1}[r_1] + p[\phi^{-1}(r_2)] \bmod I^2 \\ \Rightarrow \delta(x - [r_0]) - [r_1] + p^{p-1}[r_1] &\equiv p[\phi^{-1}(r_2)] \bmod I^2. \end{aligned} \quad (*)$$

At this point we have two different cases depending on the prime number p .

1. case: $p \geq 3$

In this case it applies that $p^{p-1} \in I^2$ and we obtain from (*) the congruence

$$\delta(x - [r_0]) - [r_1] \equiv p[\phi^{-1}(r_2)] \bmod I^2.$$

Applying δ once again and using equation (6) we have

$$\begin{aligned} \delta(\delta(x - [r_0]) - [r_1]) &\equiv \delta(p[\phi^{-1}(r_2)]) \bmod I \\ \Rightarrow \delta(\delta(x - [r_0]) - [r_1]) &\equiv [r_2] - p^{p-1}[r_2] \bmod I \\ \Rightarrow \delta(\delta(x - [r_0]) - [r_1]) &\equiv [r_2] \bmod I \end{aligned}$$

which means that

$$r_2 = \pi(\delta(\delta(x - [r_0]) - [r_1])).$$

2. case: $p = 2$

From (*) we obtain

$$\begin{aligned}\delta(x - [r_0]) + [r_1] &\equiv 2[\phi^{-1}(r_2)] \pmod{I^2} \\ (6) \Rightarrow \delta(\delta(x - [r_0]) + [r_1]) &\equiv [r_2] - 2[r_2] \pmod{I} \\ p = 2 \in I \Rightarrow \delta(\delta(x - [r_0]) + [r_1]) &\equiv [r_2] \pmod{I}.\end{aligned}$$

So we have

$$r_2 = \pi(\delta(\delta(x - [r_0]) + [r_1])).$$

For all prime numbers p the third component is given by

$$r_2 = \pi(\delta(\delta(x - [r_0]) + (-1)^p[r_1]))$$

and the isomorphism α_3 is determined by

$$\alpha_3(x) = (\pi(x), \pi(\delta(x)), \pi(\delta(\delta(x - [\pi(x)]) + (-1)^p[\pi(\delta(x))]))). \quad (12)$$

The same method can be used to determine the isomorphism α_4 for all prime numbers p . Already in this case the formulas for the small primes $p = 2$ and $p = 3$ are quite complicated. For general $n \geq 2$ we therefore concentrate on the primes $p \geq n$. Here is the main result:

Theorem 3. *For $n \geq 2$ and $p \geq n$ the ν -th Witt vector component r_ν of an element $x \in \mathbb{Z}R/I^n$ under the isomorphism $\alpha_n: \mathbb{Z}R/I^n \xrightarrow{\sim} W_n(R) = R^n$ is recursively given by*

$$r_\nu = \pi(\delta(\cdots \delta(\delta(x - [r_0]) - [r_1]) \cdots - [r_{\nu-1}])) \quad \text{for } \nu = 1, \dots, n-1$$

with the 0-th component being $r_0 = \pi(x)$.

Proof. By formula (1) the elements $r_0, \dots, r_{n-1} \in R$ are uniquely determined by the formula

$$x \equiv \sum_{k=0}^{n-1} p^k [\phi^{-k}(r_k)] \pmod{I^n} \quad \left(\in \mathbb{Z}R/I^n \right).$$

To calculate the components, we proceed inductively. In the following we use equations (6) and (10) to calculate the ν -th component r_ν for $\nu = 0, \dots, n-1$. By reducing modulo $I^{\nu+1}$ we obtain

$$x \equiv \sum_{k=0}^{\nu} p^k [\phi^{-k}(r_k)] \pmod{I^{\nu+1}}.$$

For $\nu = 0$ we are done by applying π . Otherwise we continue as follows:

Step 1: By subtracting the first term on the right-hand side we have

$$x - [r_0] \equiv \sum_{k=1}^{\nu} p^k [\phi^{-k}(r_k)] \pmod{I^{\nu+1}}.$$

Step 2: We now use equation (6) to obtain

$$\delta(x - [r_0]) \equiv \delta\left(\sum_{k=1}^{\nu} p^k [\phi^{-k}(r_k)]\right) \bmod I^{\nu} \equiv \delta\left(p\left(\sum_{k=1}^{\nu} p^{k-1} [\phi^{-k}(r_k)]\right)\right) \bmod I^{\nu}.$$

Step 3: Because of our assumption $p \geq n$ we can use equation (10) to obtain

$$\begin{aligned} \delta(x - [r_0]) &\equiv \phi\left(\sum_{k=1}^{\nu} p^{k-1} [\phi^{-k}(r_k)]\right) \bmod I^{\nu} \\ &\equiv \sum_{k=1}^{\nu} p^{k-1} [\phi^{-(k-1)}(r_k)] \bmod I^{\nu} \\ &\equiv \sum_{k=0}^{\nu-1} p^k [\phi^{-k}(r_{k+1})] \bmod I^{\nu}. \end{aligned}$$

By repeating these three steps $(\nu - 1)$ -times we finally have

$$[r_{n-1}] \bmod I \equiv \delta(\cdots \delta(\delta(x - [r_0]) - [r_1]) \cdots - [r_{n-2}]).$$

This implies the assertion by using the natural projection π and $I = \ker(\pi)$. \square

Remark 4. Comparing Theorem 3 for $n = 2$ and formula (11) we get

$$\pi(\delta(x)) = \pi(\delta(x - [\pi(x)])).$$

This can also be seen directly.

References

- [1] J. Cuntz and C. Deninger. An alternative to Witt vectors. *Münster Journal of Mathematics*, 2013. arXiv:1311.2774.
- [2] J. Cuntz and C. Deninger. Witt Vector Rings and the Relative de Rham Witt Complex. 2014. arXiv:1410.5249.
- [3] M. Hazewinkel. *Witt Vectors, Part 1*. 2007. arXiv:0804.3888.
- [4] J. Rabinoff. The Theory of Witt Vectors. 2014. arXiv:1409.7445.
- [5] J.-P. Serre. *Local fields*, volume 67 of Graduate Texts in Mathematics. Springer-Verlag, 1979. Translated from the French by Marvin Jay Greenberg.

WESTFÄLISCHE WILHELMS-UNIVERSITÄT, FACHBEREICH MATHEMATIK,
EINSTEINSTRASSE 62, 48149 MÜNSTER, GERMANY

E-mail address: sina dot ghassemi-tabar at uni-muenster dot de